

IN THE CLAIMS:

Please cancel Claims 1-18 without prejudice to or disclaimer of the recited subject matter.

Please add new Claims 19-24 as follows:

1. - 18. (Canceled)

19. (New) A system that authenticates whether or not image data included in an image file has been altered, said system comprising:

a control unit that classifies the image file into a first group if authentication data included in the image file has been generated using a private key cryptosystem, and classifies the image file into a second group if the authentication data included in the image file has been generated using a public key cryptosystem,

wherein said control unit authenticates whether or not the image data included in the image file has been altered using the authentication data included in the image file,

said control unit displays an indication of whether or not the image data included in the image file has been altered in a display area corresponding to the first group, if the image file is classified in the first group, and

said control unit displays an indication of whether or not the image data included in the image file has been altered in a display area corresponding to the second group, if the image file is classified in the second group.

20. (New) The system according to claim 19, wherein said control unit displays information related to the image file in a display area corresponding to the first group, if the image file is classified in the first group, and

said control unit displays information related to the image file in a display area corresponding to the second group, if the image file is classified in the second group, and

wherein the information related to the image file includes at least one of a thumbnail image, a file name, and a camera ID, the camera ID indicating a unique identifier of a digital camera that generated the image file.

21. (New) A method of authenticating whether or not image data included in an image file has been altered, said method comprising the steps of:

classifying the image file into a first group if authentication data included in the image file has been generated using a private key cryptosystem;

classifying the image file into a second group if the authentication data included in the image file has been generated using a public key cryptosystem;

authenticating whether or not the image data included in the image file has been altered using the authentication data included in the image file;

displaying an indication of whether or not the image data included in the image file has been altered in a display area corresponding to the first group, if the image file is classified in the first group; and

displaying an indication of whether or not the image data included in the image file has been altered in a display area corresponding to the second group, if the image file is classified in the second group.

22. (New) The method according to claim 21, further comprising the steps of:

displaying information related to the image file in a display area corresponding to the first group, if the image file is classified in the first group, and

displaying information related to the image file in a display area corresponding to the second group, if the image file is classified in the second group,

wherein the information related to the image file includes at least one of a thumbnail image, a file name, and a camera ID, the camera ID indicating a unique identifier of a digital camera that generated the image file.

23. (New) A computer-readable medium that stores a program for causing a computer to perform a method of authenticating whether or not image data included in an image file has been altered, the method comprising the steps of:

classifying the image file into a first group if authentication data included in the image file has been generated using a private key cryptosystem;

classifying the image file into a second group if the authentication data included in the image file has been generated using a public key cryptosystem;

authenticating whether or not the image data included in the image file has been altered using the authentication data included in the image file;

displaying an indication of whether or not the image data included in the image file has been altered in a display area corresponding to the first group, if the image file is classified in the first group; and

displaying an indication of whether or not the image data included in the image file has been altered in a display area corresponding to the second group, if the image file is classified in the second group.

24. (New) The computer-readable medium according to claim 23, wherein the method further comprises the steps of:

displaying information related to the image file in a display area corresponding to the first group, if the image file is classified in the first group, and

displaying information related to the image file in a display area corresponding to the second group, if the image file is classified in the second group,

wherein the information related to the image file includes at least one of a thumbnail image, a file name, and a camera ID, the camera ID indicating a unique identifier of a digital camera that generated the image file.